Cyber policing and Cyber Crime Investigation in India: Issues, Challenges and preparedness with special reference to National Capital Territory of India

A

SYNOPSIS

(THESIS PROPOSAL)

SUBMITTED TO

THE ICFAI University Dehradun

IN PARTIAL FULFILLMENT OF THE REQUIREMENT

FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY (Ph.D.)

IN

Law

BY

KOMAL ROHILLA

(Enrollment No: RSILS220007)

Under the Supervision of

Dr. MONICA KHAROLA & Dr. RAZIT SHARMA

ICFAI Law School
The ICFAI University, Dehradun
2026

The ICFAI University, Dehradun

Candidate's Declaration

I, **Komal Rohilla**, declare that the synopsis entitled, "**Cyber policing and Cyber Crime Investigation in India: Issues, Challenges and preparedness with special reference National Capital Territory of India**" being submitted in the partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in **Law** under ICFAI Law School, The ICFAI University, Dehradun during the academic year **2025-26**.

It is the work that is expected to carried out under the supervision of **Dr. Monica Kharola** and **Dr. Razit Sharma**. It is further declared that the synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

Rohilla

Signature

Komal Rohilla

Date: 26.02.2026

The ICFAI University, Dehradun

CERTIFICATE

This is to certify that the thesis entitled, **"Cyber policing and Cyber Crime Investigation in India: Issues, Challenges and preparedness with special reference National Capital Territory of India"** is an original piece of work done by ***Komal Rohilla*** under my supervision being submitted in the partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in **Law** under ICFAI Law School, The ICFAI University, Dehradun during the academic year 2025-26.

Further, it is It is certified that the synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

28/02/2026

Signature of the Co-Supervisor
Dr. Razit Sharma
Assistant Professor
ICFAI Law School
ICFAI University Dehradun

Signature of the Supervisor
Dr. Monica Kharola
Associate Professor
ICFAI Law School
ICFAI University Dehradun

ICFAI
UNIVERSITY
DEHRADUN

ICFAI University Dehradun

Certificate of Plagiarism Check for Synopsis

Author Name	KOMAL ROHILLA
Course of Study	Ph D (Law)
Name of Guide	Dr Monica Kharola & Dr Razit Sharma
Department	ICFAI Law School
Acceptable Maximum Limit	10
Submitted By	research@iudehradun.edu.in
Paper Title	Cyber Policing and Cyber Crime Investigation in India: Issues, Challenges and preparedness with special reference to National Capital Territory of India
Similarity	3%
Paper ID	5266111
Total Pages	30
Submission Date	2026-02-13 10:19:04

Signature of Student

Signature of Co-Guide

Signature of Guide

* This report has been generated by DrillBit Anti Plagiarism Software

Table of Contents

Candidate Declaration		**i**
Certificate		ii
Plagiarism report		iii
Abstract		v
1.	Introduction	1-10
2.	Research Problem	10
3.	Literature Review	11-18
4.	Research Gap	19
5.	Research Objectives	19-20
6.	Research Questions	20
7.	Hypothesis	20
8.	Research Methodology	20-21
9.	Expected Outcome	21-22
10.	Research Design	22-23
11.	Proposed Chapterization	23-24
12.	Bibliography	25-28

ABSTRACT

Cyber policing and cybercrime investigation in India have become critical areas of focus in the contemporary digital age, where the rapid expansion of internet connectivity and the increasing dependence on digital infrastructure have brought with them a parallel surge in cyber-related crimes. Particularly in the National Capital Territory (NCT) of Delhi, which serves as a hub for administrative, financial, and political activities, the challenges of policing cyberspace have been amplified due to its dense population, high internet penetration, and strategic significance. The dynamic nature of cybercrime—ranging from financial frauds, identity theft, phishing attacks, and ransomware to cyberstalking and online child abuse—demands a specialized, technologically advanced, and responsive policing system. However, the Indian law enforcement machinery continues to grapple with several issues in effectively tackling cybercrime. One of the primary challenges is the shortage of adequately trained personnel with the technical expertise to investigate digital crimes, compounded by insufficient infrastructure and outdated investigative tools in many police stations. Moreover, jurisdictional ambiguity in cybercrime cases, where perpetrators often operate from remote or international locations, adds a layer of complexity in prosecuting offenders. The legal framework, though evolving, is still playing catch-up with the fast pace of technological innovation. While the Information Technology Act, 2000 and provisions in the Bhartiya nyaya Sanhita, 2023 provide a foundational legal basis, gaps remain in areas such as data privacy, cross-border data access, and cyber forensics.

In the context of the NCT, despite the establishment of dedicated cyber cells and the implementation of initiatives like the Cyber Safe Delhi campaign, coordination between various agencies—state police, central enforcement bodies, judiciary, and private stakeholders—remains inconsistent and fragmented. The general public's limited awareness about cyber threats and poor digital hygiene also contribute to the growing number of cybercrime incidents, making prevention efforts less effective. Preparedness, both in terms of policy and on-ground enforcement, is still evolving. While recent years have witnessed greater investment in capacity-building programs, establishment of cyber labs, and partnerships with technology companies for knowledge exchange, much more remains to be done in terms of upgrading cyber intelligence, enhancing inter-agency data sharing, and framing comprehensive protocols for incident response and digital evidence management.

Furthermore, the judicial process related to cybercrime often suffers from delays due to the lack of specialized knowledge among legal professionals, leading to low conviction rates. In a

rapidly digitalizing India, especially in key urban centers like Delhi, it is imperative to adopt a multi-stakeholder approach involving government bodies, tech experts, academic institutions, and civil society to formulate a resilient cyber governance framework. Holistic reforms—ranging from legal amendments and strategic investment in technology to awareness campaigns and international cooperation—are essential for empowering cyber policing mechanisms and ensuring that law enforcement can match the sophistication of cybercriminals. Addressing these multifaceted challenges with a strategic, forward-looking approach will be key to safeguarding India's digital future and maintaining public trust in digital systems, particularly in the high-stakes environment of the National Capital Territory.

Key Words: Bhartiya Nagarik Suraksha Sanhita, 2023; Digital Personal Data Protection Act 2023; National Cyber Security Policy; The Indian Cyber Crime Coordination Centre (I4C); National Cyber Crime Reporting Portal

1. INTRODUCTION

BACKGROUND

The digital revolution in India with over a billion internet users has been accompanied by a parallel rise in cybercrime. Cyber offenses now range from traditional crimes (theft, fraud, defamation, harassment, etc.) perpetrated through electronic means to novel "new age" offenses peculiar to the digital realm (hacking, identity theft, malware, cyber-terrorism, online sexual exploitation, etc.). In simple terms, a cybercrime involves unlawful acts where a computer or network is either the target or the instrument of crime. For example, "computers as targets" covers hacking, denial-of-service attacks and virus propagation, whereas "computers as weapons" covers crimes like online fraud, phishing, intellectual property violations and distribution of obscene content. In the Indian context, early cyber incidents (late 1990s/early 2000s) involved rudimentary hacking and credit-card frauds, but by the 2010s cyber criminals were deploying sophisticated scams, ransomware, social-engineering tricks (such as "Digital Arrest" or fake regulatory calls) and exploiting social media. High-profile cases (e.g. the 2001 "Sony.sambandh.com" online fraud) illustrated the need for cyber-specific laws. Over time cyber offenses have proliferated: complaints to India's cyber coordination centre rose almost six-fold from about 26,000 in 2019 to over 1.59 million in 2023.

Analysts note that traditional fraud and impersonation schemes have morphed into massive social engineering networks, while crimes like child sexual abuse material and online defamation have surged. Thus, cybercrime in India today is understood as encompassing any unlawful act aided by an electronic system – for instance identity theft (IT Act, Section 66C), fraudulent personation (Section 66D), privacy violations (Section 66E), spreading obscene or pornographic material (Section 67–67B), and even cyber-terrorism (Section 66F) as well as traditional offences (IPC Section 420, 409, etc.) carried out via computers.

The Information Technology Act, 2000 (as amended) and **the Indian Penal Code, 1860** or **Bhartiya Nyaya Sanhita, 2023** form the core of India's cyber law framework. The IT Act was India's first comprehensive cyber law: it recognizes electronic records and digital signatures, empowers authorities to regulate cyber infrastructure, and expressly creates new offences. Its Chapter XI lists key cyber offences: for example, Section 66C–66F criminalize identity theft, cheating by electronic personation, privacy violation, and cyber-terrorism. Section 67 and its subsections penalize publication or transmission of obscene or sexually explicit material

(including child pornography) in electronic form. The Act also confers broad investigative powers: e.g. police may search computers and seize evidence (section 80) and the Act has "overriding effect" over other laws (section 81). Particularly, Section 75 extends jurisdiction to cover offences committed abroad if they involve a computer resource located in India. (In fact, Sec.75 is broader than IPC jurisdictional rules: it allows prosecution for any cyber offence where the targeted computer is in India.) Over time, the IT Act has been amended to address new concerns. 'The IT (Amendment) Act, 2008' added many provisions: for example, Section 66A (punishing sending of "offensive" online messages) was later struck down by the Supreme Court, but the amendment also introduced powers to block websites (Sec.69A) and preserve critical data (Sec.69).

In 2008 the Act was further updated by the CrPC Amendment to create the Examiner of Electronic Evidence (Section 79A) to standardize digital forensics. More recently, rules under the Act (such as the 2021 Intermediary Guidelines) oblige online platforms to report incidents and takedown illegal content within strict timelines. 'The Digital Personal Data Protection Act 2023' (stemming from the 2019 draft Personal Data Protection Bill) also impacts cybercrime investigation, as it regulates processing of personal data and mandates security safeguards.

Meanwhile, the IPC and allied laws have been amended to cover cyber-enabled offences. For example, Sections 354A–354D of the IPC (introduced in 2013–2018) broaden sexual harassment laws to include cyber-harassment and stalking: Section 354A(d) explicitly covers making offensive comments via email or phone, and Section 354D(1)(ii) defines "cyberstalking" as repeated contact or monitoring using electronic communication. Section 507 criminalizes intimidation by anonymous communication (e.g. frightening email threats), and Section 509 covers insults to modesty by any form of communication. Section 188 IPC (disobedience of government order) is sometimes invoked in cyber contexts (e.g. ignoring lawful takedown requests). Additionally, the Protection of Children from Sexual Offences (POCSO) Act, 2012 penalizes use of children in digital pornography, and CrPC Section 114A extended defamation laws by allowing civil suits in any jurisdiction where defamatory content is published online. In short, the legislative regime for the cybercrimes is a hybrid: new provisions in the IT Act work along with traditional IPC offences adapted to digital modus operandi.

In the meantime, with the swift growth of the digital technologies, women in India are increasingly facing targeted cybercrimes such as online harassment, cyberstalking, non-consensual sharing of images, and trolling etc. These crimes not only threaten their privacy and

dignity but also raise serious concerns about their digital safety and human rights as well. In response to this growing challenge, institutions like the National Commission for Women (NCW) and the National Human Rights Commission (NHRC) have emerged as key stakeholders in addressing and redressing cybercrimes against women. Their roles encompass the policy advocacy, grievance redressal, awareness generation, and coordination with law enforcement agencies to ensure that the women's rights are protected in the digital realm.

1.1. Legislative Legal Framework (Key Laws and Amendments)

1.1.1 Information Technology Act, 2000: This Act establishes the electronic commerce/legal recognition of digital records and signatures, and creates cyber offences. Relevant provisions include: Section 43 (penalty for data damage/theft), Section 66 (general computer offences), Section 66A (no longer in force, struck down), Section 66B–66E (dishonestly receiving stolen devices, identity theft, cheating by personation, invasion of privacy) Section 66F (cyber-terrorism)

Sections 67, 67A and 67B punish publishing/transmitting obscene or sexually explicit material online. Section 69 empowers authorities to intercept/monitor or decrypt information for national security; Section 69A allows blocking of online content by government order; Section 69B allows collection of traffic data for cybersecurity, Section 75 explicitly extends the Act to cyber-offences committed outside India if the computer system involved is in India.

30

1.1.2 Indian Penal Code, 1860: Many IPC sections apply when offences use computers as a means. For instance, fraud and cheating (IPC Section 420, 415, 465 etc.) are invoked for online banking scams; theft (Section 378) applies to stealing digital assets; forgery (Section 463) covers fake electronic documents.

In recent years, the IPC has been amended to address technology-specific behaviour: Section 354A(d) forbids repeated electronic communication with sexual intent, Section 354D(1)(ii) defines cyberstalking as persistent contact via any form of electronic media, Section 507 punishes anonymous threat via letters or telegrams, and Section 509 criminalizes sending indecent or insulting message. These all amendments were somewhat a response to crimes like 'revenge pornography' and online harassment. Also, another important provision that was applied during Covid-19 lockdown was to penalize the violation of regulatory orders that was communicated electronically. Other legislations, including the POCSO and the Indian Evidence

Act also have an effect on cyber offences in that they deal with digital evidences and sexual exploitation.

1.1.3 Bhartiya Nyaya Sanhita, 2023: The Bhartiya Nyaya Sanhita 2023, this act replaces the colonial era that is Indian Penal Code 1860, it marks a substantial legislative advancement in India's criminal justice system, especially in addressing present-day challenges such as Cybercrime. The BNS brings Indian law into the digital age now. It directly addresses modern crimes like Cyberstalking, identity theft, and sharing harmful content online.

Section 69 of BNS specifically targets identity theft committed through electronic means. Chapter VI deals with serious threats to the state, including cyber terrorism. NCT of Delhi faces a particularly high number of cybercrimes. This is because of its advanced digital infrastructure and large population. The BNS gives law enforcement strong legal tools to investigate and prosecute these cases. However, implementing the new law comes with challenges. Cyber Police need continuous training to keep their skills updated. Forensic labs need better technology and resources. Officers must learn proper methods for collecting digital evidence and ensuring it can be used in court. Delhi's cyber policing units, especially the cyber crime unit of Delhi Police, must be fully prepared. Their readiness is crucial for the law to work effectively. Success also depends on other factors also. The public needs to be aware and willing to cooperate, different agencies must coordinate with each other. Courts and judges need to understand digital crimes. All these elements working together will help India tackle evolving cyber threats.

.

1.1.4 Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection (DPDP) Act, 2023 plays a crucial role in strengthening the framework for cyber policing and cybercrime investigation in India by introducing robust data protection standards and accountability mechanisms. Basically, the primary object of this Act is to safeguard the digital personal data. Whereas, it has important implications also for law enforcement, cybercrime prevention, and the protection of the citizens especially the vulnerable groups from digital threats.

The significant role of the DPDP Act in cyber policing is that it focuses on the idea that the data processing is done in contests. Also, the privacy of the personal data cannot be collected, stored or shared without the consent of the individual. The immediate effect of this can be seen in the cases of illegal data collection, doxxing and the identity theft. As these are the common cases of cybercrime that is related to women This has made the police force have a strong authority to be aggressive against platform/people who abuse personal data which has now become clear with

this Act. Particularly clear in terms of definition as well as penalty of Violations.

The DPDP Act requires data fiduciaries to maintain reasonable security standards. This helps prevent data breaches. Organizations that fail to comply face significant penalties. The Act serves as a strong deterrent against careless handling of personal information. Such negligence often leads to cybercrimes like phishing, stalking, and online extortion. The DPDP Act provides crucial legal support to digital law enforcement units. This includes specialized teams like the CyPAD unit of Delhi Police. These units are responsible for protecting citizens in the digital space. The Act also established the Data Protection Board of India. This board has important powers and responsibilities, also they can investigate data breaches and impose corrective measures on violators. The Board is not a law enforcement agency. However, it can support criminal investigations, its findings and inquiries provide valuable assistance to police and other agencies. In summary, the DPDP Act strengthens cyber policing in India in several ways like it enforces accountability for data handling, ensures processing happens only with proper consent. It mandates better security standards across organization. These provisions create a more robust framework for combating cybercrime and protecting citizens online.

1.1.5 Current Amendments and Proposals: Current developments include the IT (Amendment) Rules 2021. The Union Government has periodically amended the IT Act schedules (e.g. key definitions or penalty slabs) and continues to review stronger encryption/legal interception policies. Parliamentary committees and expert groups have proposed measures like mandatory data localization, stronger identity verification for virtual currencies, and granting law enforcement access to encrypted data (raising privacy debates). Notably, India has not joined the Budapest Convention on Cybercrime; scholars argue that without this global framework, mutual legal assistance for cross-border cyber investigation remains ad hoc and slow.

.

1.2. Key Challenges in Cyber Policing and Investigation

Cyber policing in India faces multifaceted challenges:

1.2.1 Jurisdictional Complexity: In essence, cybercrime also lack boundaries. Criminals may even be located in different states or even other countries as well, they may be using servers anywhere in the world, so they may be hard to detect and prosecute.

It is right to say that Section 75 of Information Technology Act and Sections 179-182 of the CrPC provides that the Indian courts can take cognizance of the cybercrimes that are at the

international level. Either the target has been in India or the server itself, in any case, Indian courts have to search for MLAT (mutual legal assistance treaty), which is a lengthy process. Likewise, as a non-member of the Budapest Convention, the probability of smooth handling of cybercrimes in India through international collaboration has been a very serious issue. In the meantime, according to research, accepting the international norms by India can make a huge difference in the international collaboration to handle cybercrimes.

1.2.2 Forensic Capacity Shortfall: The underfunding of the forensic services poses a problem to the law Enforcement bodies. For instance, the state Forensic Science Laboratory in New Delhi had more than 6000 pending cyber forensic cases in mid-2025. An FSL Officer, who is in a high ranking, had already been stated that they had over more than 100 cases every month, which they are not even able to look into them. The backlog of the cases is triggered even by the increased digital crimes of hard drives in computers, cell phones and surveillance videos which are primarily the result of the activities. The cyber forensic unit is especially silent and it is incapable of appropriate results because it lacks staff and require cultural equipment. And the lack of coordination between the agencies in the case of collected evidences in the form of missing data at the investigating agencies once again causes a backlog.

1.2.3 Training and Expertise Gaps: Maximum police staff has no special cyber skills. Despite the existence of units like the CyPAD of the Delhi Police which has primarily trained several 100's of officers and approx. 850 Inspectors/Sub- Inspectors. The scale of demand is much higher. Even at a national level, within the CCPWC (Cyber Crime prevention against Women and Children) Scheme of the Home Ministry, 25000 + police officers and prosecutors have been trained on the cybercrime investigation, and by the end of 2025 1lakh+ officers had registered on online CyTrain i.e. National Cybercrime Training Centre platform.

However, due to the development of cyber threats, it is necessary to continuously upgrade. Many of the states and district police departments do not have forensic departments or cyber cells and even first responders are also not trained on handling the electronic evidences. A lack of a cyber crime investigators and analysts is also a significant gap.

1.2.4 Privacy and Legal Constraints: Investigations must balance efficacy with civil liberties. The Supreme Court's 2017 judgment in **K.S. Puttaswamy v. UOI** affirmed that privacy is a fundamental right, which means surveillance or data collection in cybercrime probes must have legal authorization and safeguards. Constitutional constraints and concerns about intrusive laws can limit quick police action (e.g. requiring warrants to access emails or encrypted phones). Recent controversies over mandatory data retention (such as CERT-In rules requiring companies to report breaches rapidly) illustrate the tension between regulation and privacy. Thus, designing

lawful investigation techniques (digital searches, metadata analysis, lawful interception) while respecting individual rights is an ongoing challenge for Indian cyber policing.

1.2.5 International Cooperation and Diplomacy: Cybercrimes often involve foreign nationals or servers abroad (e.g. spam, phishing call centres, crypto scams). Extradition of cyber offenders is rare and relies on diplomatic processes. Although India works bilaterally and via INTERPOL to track cyber criminals, it lacks a dedicated fast-track mechanism. Experts argue that India should ratify global treaties (like the Budapest Convention) and strengthen its Mutual Legal Assistance framework to improve cybercrime cross-border enforcement.

1.3. Cyber Policing in Delhi: Preparedness and Initiatives

The National Capital Territory (NCT) of Delhi with its dense population and status as the seat of government has seen especially active measures against cybercrime. Delhi Police has developed a special cell under its cyber cell called 'The Intelligence Fusion and Strategic Operations' i.e. IFSO. This unit is called CyPAD (Cyber Prevention Awareness and Detection)

And has the mandate to investigate complex cybercrimes specially those which are committed the vulnerable section of our society i.e. women and children. This CyPAD has National Cyber Forensic Lab (NCFL) which is capable of retrieving deleted information. For example, information from hard drives, mobile phones, create forensic images and even restore certain information on the Androids, iOS etc.

In Delhi, CyPAD heads cyber awareness and capacity building. It creates systematic educational courses regarding online safety, and holds workshops in schools, colleges around Delhi. This unit is even equipped with more than 80 inspectors and sub inspectors of the district cyber cells and police stations on cyber investigation techniques.

Moreover, Delhi Police actively disseminate cyber safety information on its websites and social media (e.g. Cyber Safety tips for children, women, etc. are published and videos shared) Public outreach campaigns (often in partnership with academia and industry) aim to educate citizens about phishing, e-banking safety, social media hygiene and fraud prevention.

In case of infrastructure Delhi benefits from a number of central initiatives in place. The Union Home Ministry's I4C (Indian Cyber Crime Coordination Centre) is headquartered in New Delhi. Under I4C, a national Cyber Crime Reporting Portal (cybercrime.gov.in) allows any citizen to file complaints online for all types of cybercrimes. The Cases reported on this portal, used regularly by the Delhi Police cyber unit, and are routed to the relevant local agencies for strict

action.

The Indian Cybercrime Coordination Centre (I4C) established a new facility in New Delhi. It is called the National Cyber Forensic Laboratory. The lab's primary purpose is to provide forensic support to police officers across India. The National Lab is separate from Delhi's own forensic However, Delhi's state forensic labs face a major problem i.e. they have a massive backlog of cases waiting for analysis. Thia leads to significant delays in investigations.

Many cases depend on the National Lab or external specialists for forensic analysis. Delhi's own cyber forensic capabilities urgently need upgrading. To address these gaps, the Ministry of Home Affairs took action under the cyber crime Prevention against Women and Children (CCPWC) scheme, they funded a new facility in Delhi. This facility serves dual purpose as both a cyber forensic lab and a training centre. This investment aims to strengthen Delhi's capacity to handle cybercrimes more quickly and effectively. Also trained more than thousands of staff under this scheme. However additional works were needed to make sure that the progress is as the same as of cyber criminals.

1.4. National Cyber Institutions and Initiatives

In India there has been some major development of multiple layered institutional structure in relation to cyber policing and cybersecurity in India. First one is the I4C i.e. Indian Cyber Crime Coordination Centre under the ministry of Home Affairs which is considered as a nodal body to empower all the activities related to cyber crime across the whole country. This body was launched in 2020 and it comprises of number of units like threat analytics, training, research and Joint Cyber Coordination Teams. Besides this the most important elements are the National Cyber Crime Reporting Portal and the banking/financial cyber fraud reporting system of citizen i.e. Helpline Number 1930. Till now this National Cybercrime Reporting Portal has registered even more than a million complaints with the extensive variety of offences like fraud, harassment, child abuse material etc.

Under this Indian Cyber Crime Coordination Centre, the government has launched numerous capacity building and the awareness programs also. Even a massive open online course platform, CyTrain offers modules on cyber investigation and digital forensics. Under this above 1,00,000 police personnel and judicial officers have registered for training purpose, with around 80,000 certificates are issued by late 2024. The CCPWC (Cyber Crime Prevention against Women and Children) scheme has provided approx. Rs.141. crore to states and UT's, resulting in cyber forensics and training labs in 34 jurisdictions. Through this scheme they even provided training to more than 2,00 law enforcement officers, prosecutors and judges in cyber-crime matters.

Regular peer-learning sessions for CAPFs and state police (nearly 98 sessions so far) and the creation of Joint Cyber Coordination Teams in cyber-crime hotspots (e.g. Hyderabad, Ahmedabad, Chandigarh) further strengthen national readiness. The government also actively uses media and technology for awareness: campaigns (SMS alerts, social media accounts like @CyberDost, radio/TV spots, Delhi Metro ads on "digital arrest" scams, etc.) aim to educate citizens about common cyber threats.

A parallel institution is **CERT-In** (Indian Computer Emergency Response Team) under the Ministry of Electronics & IT, India's national agency for cybersecurity. CERT-In maintains an automated threat intelligence platform, monitoring incident reports and issuing advisories to organizations. It operates the **National Cyber Coordination Centre (NCCC)** to collect and analyse cyber threats across sectors, and the **Cyber Swachhta Kendra** (Botnet Cleaning Centre) to help citizens and companies remove malware. CERT-In also conducts cyber drills: over 100 drills involving ~1,450 entities have tested the resilience of critical infrastructure. To build skills, CERT-In has trained thousands of network/system administrators and CISOs in government and critical industries (by late 2024, over 9,800 officials were trained in 20 programs).

And if speaking about women related Cybercrimes they are also combated with the help of institutions like '*National Commission of Women'* (NCW) and '*National Human Rights Commission'* (NHRC). These institutions act as a watchdog and justice enforcer of the cyber sphere. The statutory organization National Commission of Women is established as a result of NCW Act, 1990 is slowly but definitely adjusting to the new waves and problems. And the problems are like online stalking as well as the cyber violence is inflicting on the women of our country. In addition, it serves as a path under which the survivors can complain online using its special online portal and WhatsApp complaint system so thus making it simpler and more appropriate. Even, they organise campaigns and workshops also with women and children on how to be cautious digitally and what they do online and the legal measures they may apply to these criminals. Although they lack the power of enforcing it, but they play a very significant role as a resolving force. It bridges the state police, cyber cells and online providing services in an attempt to hasten the complaints and make them accountable.

And the other one is NHRC, this commission is also interested in cybercrimes which deals with the issues of women and children in protecting their basic human rights. It essentially deals with the freedom of privacy, dignity and violence.when cybercrimes are one of the signs of a bigger issue of human rights violation such as the revenge porn, stocking and cyber defamation etc, the National Human Right Commission is entangled.

It can even call the reports of law enforcement agency and prescribe them and control the

appearance of the recommendations. The NCW and NHRC can be seen to be doing similar policy support which include proposing amendments to laws, advocating the effective enforcement of the provisions in the current laws through the 'Information technology act 2000' and creating capacity building among the law enforcement officers. These institutions together work in a complimentary manner and not only addressing individual grievances but also in affecting system change in order to make the cyberspace safer to the women and children in India.

In short, the India national cyber defence ecosystem has a specific reporting portal, special coordination Centre that is I4C, financial fraud helpline 1930, national forensic club, cyber security emergency team (CERT-IN), and massive training/ awareness initiatives. so, these agencies are the supplementary to state and District policing.? For an instance, the cyber cell in Delhi is closely aligned with CERT-IN and NCC on threat warning and issues the NCFL and training material at the I4C. At the same time, the legislative changes (example the IT rules 2021 on breach reporting) and the appearance of new organisations such as the office of national cyber security coordinator are supposed to make the law enforcement instruments sharper even. India is attempting to develop strong cyber policing by combining all the legal authority all the special agencies and capacity building but still there are crucial gaps. These dimensions will be discussed in detail in this thesis with the aim of determining the extent to which Delhi is ready to combat cyber-crime and the lessons what it has learnt about what the country can learn.

.

2. Research Problem-

The Effective coordination of the Delhi Police Cyber Cell, CERT-In, NCIIPC with the state or central law enforcement agencies in real time investigation of cybercrimes is lacking. The Information Technology Act 2000 and its further revisions are no longer enough to address the emerging cyber threats, namely AI- generated crimes, ransomware-as-a-service (Raas), deepfakes, darknet transactions and cryptocurrency frauds. It is very common with the policemen and investigators who have not been trained in cyber forensics, handling of digital evidence, and the interpretation of cyber laws in the courts.

Number of cybercrimes cases are not handled by using data-driven technologies such as cyber intelligence software, behavioral analytics, and even AI based surveillance but by the old conventional policing techniques. The cyber police units of Delhi have begun to use digital tools, although in an uneven manner due to the budget cuts. The cases of Cybercrimes in which actors are located or servers are located beyond India are characterized by delays in the

procedures through the absence of Mutual Legal Assistance Treaties (MLATs) and the non-membership in the Budapest convention.

3. Literature Review

The literature Review of my tentative thesis topic covered number of Research papers, books, and Reports but I mentioned below certain selected literature with international, national, and regional aspects as Follows-

- The Author Raghavan, R. in the article **"***Cybercrime, Policing, and Public Trust"* This study explores the relationship between public trust and cybercrime reporting in metropolitan cities, including Delhi. It notes that mistrust in police efficiency, fear of stigma, and digital illiteracy discourage reporting of cybercrimes like cyberstalking and online fraud.

  Research Gap: The study is broad and urban-focused but lacks granular insights into Delhi's specific cyber units or case outcomes. Future studies could analyze whether public trust initiatives (like Delhi Police's CyPAD awareness campaigns) improve citizen reporting.

- The Authors Sen, S. & Thomas, D. in the article "*Assessing the Cybercrime Capacity of Indian Law Enforcement"*. Using structured interviews with officers from Delhi, Mumbai, and Bengaluru, this study evaluates cybercrime knowledge among mid-level investigators. It finds significant gaps in digital evidence handling, inconsistent training across states, and lack of specialization.

  Research Gap: Although it includes Delhi, the study does not differentiate by unit (e.g., CyPAD vs local stations). There's a need for in-depth study on intra-city disparities in training and tech capability within Delhi.

- The Authors Sharma, K. & Iyer, A. in the article "*Digital Gender Harassment in India: Police Response and Legal Challenges".* examines law enforcement response to digital harassment and revenge porn, particularly in Delhi and Haryana.

  Research Gap: While it covers Delhi, the focus is on victim experience rather than law enforcement policy. More research is needed on whether institutional reforms (e.g., gender-sensitized cybercrime desks) are implemented effectively and impact outcomes.

- The Author Patel, N in the article "*Judicial Trends in Cybercrime: Balancing Privacy and State Surveillance.*". This doctrinal analysis reviews landmark cases like K. S Puttaswamy (privacy), Shreya Singhal (free speech), and newer lower court judgments

involving digital surveillance. It finds courts increasingly demand proportionality and legality in digital search/seizure.

Research Gap: It lacks application to investigation practice—how these rulings influence actual Delhi Police procedures or forensic data handling is not discussed. Empirical legal research could bridge this theory-practice divide.

- The Author Verma, A in his Book "*Role of National Cyber Coordination Centre in Investigations. Indian Police Journal"* outlines how the NCCC and CERT-In feed intelligence to Delhi and other state cyber cells. It explains protocols for sharing metadata, phishing alerts, and coordinated takedowns.

  Research Gap: While descriptive, it doesn't evaluate how timely or actionable the intelligence is. A performance audit or satisfaction survey from Delhi Police units would add critical depth.

- The Authors Rao, S. & Khan, in this article "Juvenile Involvement in Cybercrime: A New Threat". Focused on NCR, this study highlights the rise in cyber offences by minors, especially in Delhi's suburban zones. The paper raises concerns about the lack of preventive education and reformative justice options.

  Research Gap: The study does not assess how Delhi Police or CyPAD are adapting juvenile justice protocols for online crime. Future research could analyze police–school collaboration and early intervention efficacy.

- The Authors Ahmed, F. & Sengupta, A in this article "*Comparative Study of Cyber Policing in India and South Korea"* contrasts India's decentralized cyber policing with South Korea's centralized KISA model. It notes how Korea's streamlined cyber units outperform Indian systems in response time and citizen satisfaction.

  Research Gap: It lacks case-specific data from Delhi or implementation feasibility in Indian federal structure. Further study is needed on whether a hybrid centralized–state model could work in India's urban settings like Delhi.

- The authors Mishra, R. & Sharma, D *"Cybercrime Prosecution in India: Institutional Shortcomings and Case Delays".* In this article evaluates prosecution delays in cybercrime cases in Delhi and Mumbai. The authors highlight issues such as non-expert judges, limited cyber benches, and lack of electronic evidence training for prosecutors.

  Research Gap: While it addresses prosecution challenges, it does not consider how police investigation quality or digital forensic capacity affect case outcomes. Future research could study this linkage.

- The Author Das, in this article "The Role of Capacity Building in Strengthening Cyber

Policing in India" analyzes central schemes like the I4C, CyTrain, and CCPWC, evaluating their impact on officer readiness. A survey of 300 police officers across five states (including Delhi) showed 58% had not received formal cybercrime training.

Research Gap: The study does not measure whether trained officers resolve cases faster or better. Follow-up studies should assess training outcomes and citizen satisfaction.

- The Authors Kumari, R. & Shekhar, S. in this article "*Cyber Victimology and Reporting Patterns Among Women in Urban India*" surveyed women victims of cyberstalking and image abuse in Delhi and Bengaluru. Only 18% filed official complaints. Barriers included social stigma, lack of trust in police, and limited cyber awareness.

  Research Gap: There is little exploration of how police responsiveness (e.g. CyPAD's outreach in Delhi) affects reporting. Future work could examine institutional trust-building.

- The Author Rathore, A in this article "*Evaluating the Role of Delhi Police Cyber Cell in Financial Cybercrime Investigations*". This case study assesses CyPAD's use of the 1930 helpline and financial fraud response system. He finds that while reporting efficiency improved, evidence retrieval from banks and fintech companies remained slow.

  Research Gap: The study lacks user-side feedback. Future studies should assess victim satisfaction and recovery rates post-reporting.

- The Authors Saxena, P. & Bhardwaj, V in this article "*Inter-Agency Coordination in Tackling Online Child Sexual Exploitation in India".* This article investigates coordination between Delhi Police, NCPCR, and INTERPOL in cases of child sexual abuse material (CSAM). Delays often occur due to jurisdictional gaps, poor data localization, and slow ISP responses.

  Research Gap: The paper recommends better treaties and tech integration, but lacks input from field investigators. Further research could collect interviews or track CSAM case timelines.

- The Author Agarwal, K. in this article *"Legal Reforms and the Bhartiya Nyaya Sanhita: A New Era in Cybercrime Regulation?"* article critically evaluates the shift from IPC to BNS, noting the inclusion of identity theft, online obscenity, and cyber fraud under clearer sections. Agarwal applauds the legal codification but warns about enforcement limitations.

  Research Gap: It's a legal critique without empirical insight into police or judicial readiness for implementing BNS. Future research could assess training alignment and case classification consistency post-reform.

- The Author Mehta, S. "*Cyber Forensics in India: Gaps Between Policy and Practice"* finds that although digital forensics is recognized under the IT Act and CrPC, labs are underfunded, with case backlogs exceeding 6–12 months in Delhi.

  Research Gap: No tracking is done of how this delay impacts convictions. Research could focus on the chain-of-custody breakdowns and trial timelines.

- The Authors Tiwari, P. & Yadav, in this article N. *"Judicial Trends in Cybercrime Jurisprudence Post-Puttaswamy"*. The article reviews SC and Delhi HC judgments on privacy, digital searches, and online free speech. It finds courts often oscillate between national security and civil liberties.

  Research Gap: There's no review of how lower courts apply these doctrines during bail hearings or trials. Future work could analyze trial court judgments on search and seizure in cyber cases.

- The Authors Sood, A., Aggarwal, S., & Singh, S. in this article "*Analysis of Digital Forensic Practices in India"* based on interviews with digital forensic scientists and police, this study reveals that most Indian forensic labs handle far fewer cases than assumed, and official statistics are incomplete. It identifies systemic gaps: lack of a regulatory authority, inconsistent procedures, accreditation shortfalls, and insufficient training. The authors propose concrete reforms – e.g. establishing a forensic oversight body, international evidence-sharing treaties, uniform forensic standards, and private-sector accreditation of labs. The contribution is a practitioner-driven audit of India's forensic capacity.

  Research Gap: Its limitation is the scarce data (many labs did not report), so the findings are mainly qualitative; it points to a need for comprehensive quantitative studies on lab workloads and case backlogs.

- Th Authors Attri, S. A., Jaiswal, R., Jaiswal, S., & Baggan, J in this article "*The Role of Six States' Police in Mitigating Cyber Crime in India*". This comparative case-study article examines how six states (including Delhi) tackled specific cybercrime incidents. For Delhi, it describes how the Cyber Crime Unit arrested online harassers by partnering with social media platforms and launched public safety campaigns. It notes persistent challenges: cybercriminals crossing jurisdictions, privacy issues in evidence, and slow legal processes. In Madhya Pradesh (2023 case), it finds limited public awareness and forensic tools, plus jurisdictional barriers that "discourage victims from reporting crimes". The authors recommend expanded awareness programs, advanced training and labs, and stronger inter-state/international collaboration.

Research Gap: its insights are concrete but not generalizable; it highlights the need for systematic surveys of citizen reporting behavior and measurable evaluation of these police initiatives.

- The Author Rani, M. in this article "*Impacts and Ethics of Using Artificial Intelligence (AI) by the Indian Police"* reviews secondary sources to assess India's nascent use of AI (e.g. facial recognition, crime mapping) in policing. She argues AI can enhance efficiency – e.g. by predicting crime and identifying suspects with fewer resources – but cautions that algorithmic bias can replicate societal prejudices (noting factors like caste, religion). The paper highlights India's push for AI despite ethical conflicts and calls for careful policy and public scrutiny. Its contribution is raising awareness of AI ethics in Indian policing.

  Research Gap: The gap is that it relies on literature rather than primary data; it suggests the need for empirical studies on actual AI deployments in Indian law enforcement and how they affect fairness and public trust.

- The Authors Bhaskaran, P. & Gole, Y in this article "*Adjudicating and Investigating Cross-Border Cybercrimes: A Study of India's Jurisdictional Framework"* analyzes India's legal regime for extraterritorial cybercrime. It notes that recent legislation (IT Act 2000, Bharatiya Nagrik Suraksha Sanhita 2023, etc.) nominally empowers Indian courts over overseas cyber offenses. However, in practice India still must rely on slow mutual legal assistance treaties and international cooperation, leading to gaps in prosecuting transnational offenders. The authors highlight issues like India's non-participation in the Budapest Convention and delays in evidence exchange. They propose reforms to streamline extradition and data-sharing.

  Research Gap: the authors themselves point out that empirical research is lacking: "there remains a critical gap in empirical research" on enforcement challenges, and future studies should include case analyses of cross-border investigations.

- The Author Singh, A in this article *"Digital Arrest Trends and Case Volumes in Cyber Policing"*takes a global-analytic view of cyber policing trends. Singh notes that use of advanced technologies (AI, blockchain, forensic tools) has corresponded with a steady rise in cyber-arrest volumes

  He also cites international examples (e.g. FBI operations) to emphasize cross-border cooperation. However, he warns that traditional challenges remain – resource constraints, jurisdictional disparities, privacy and bias issues – and argues for global legal harmonization and ongoing innovation in police tools. The paper's contribution is

framing cybercrime policing in a technological context.

Research Gap: Its limitation is lack of India-specific data or case studies, making its recommendations quite general and untested in the Indian setting.

- The Author Jadhav, Y.M in this article *"Analyzing Efficacy and Enhancing Accessibility: A Study of India's National Cyber Crime Reporting Portal in Addressing Financial Cybercrimes"*. This empirical study evaluates India's online portal (cybercrime.gov.in) for reporting financial cyber offenses. Using official statistics, victim surveys, and interviews with officials, it finds that the portal has improved reporting for fraud and phishing cases but still faces hurdles (such as user-unfriendliness and low awareness) that limit its impact. It offers recommendations to make the portal more user-centric and to raise public awareness.

  Research Gap: As it focuses on financial crimes, the study's scope is narrow; it notes future work should assess the portal's role in other crime categories and measure how changes (e.g. interface improvements) affect reporting rates over time.

- The Author Kumar, K. & Verma, N.K in this article "*Cyber-Financial (Cy-Fi) Fraud in India: A Case Study of COVID-19 Induced Cybercrime in Mewat Region"*. This case study examines why the Mewat region (Haryana) became a hotbed of online financial fraud during the COVID-19 lockdown. The authors link the surge in cyber-fraud to pre-existing social and economic underdevelopment (e.g. low education, joblessness) that made local youth susceptible to fraud schemes. They argue that sustainable solutions must address these socio-economic "development gaps" through education, employment programs and stricter local governance, rather than relying solely on policing. The paper's contribution is highlighting non-technical factors in cybercrime hotspots.

  Research Gap: Its limitation is its narrow focus on one rural area; the findings may not generalize, and it does not empirically test law enforcement strategies, suggesting a need for broader quantitative studies of rural cybercrime dynamics.

- The Author Khan, A.A in this article "*Reconceptualizing Policing for Cybercrime*" police deputy superintendent argues for shifting cyber policing goals away from traditional arrest-centric models to a "harm-centric" approach. He notes global trends (cybercrime ~70% of total crime in Singapore) and suggests focusing on disrupting criminal infrastructure (financial networks, illicit data flows, harmful online content) rather than only catching offenders. He emphasizes public–private cooperation and international collaboration as keys.

  Research Gap: A limitation is its lack of data or testing in India – it is a conceptual piece

– indicating a gap for empirical analysis of how such harm-focused strategies might work in the Indian context.

- The author Chavan, R.R in this article "*The Effectiveness of India's Cybercrime Investigation and Prosecution Framework in Dealing with Cybercrime Cases".* This overview essay critically examines India's cyber laws and enforcement. Although the IT Act 2000 criminalizes many online offences, most Internet users lack the technical awareness to use these laws effectively. He highlights gaps such as overly broad provisions (e.g. struck-down Section 66A) and laws that were initially aimed at facilitating business rather than victim protection. In conclusion, he observes that India has improved (through new laws, awareness drives and cyber infrastructure) but "challenges persist" – calling for continued investment in cyber capacity-building and international coordination.

  Research Gap: The paper's contribution is a general stock-taking for the lay reader. Its limitation is the anecdotal nature and lack of original data; it suggests further research into how legal reforms (like the 2023 penal overhaul) actually impact case outcomes in practice.

- The Author Iqbal, S in this article "*Blockchain-Based Evidence and Indian Courts: Legal Possibilities and Practical Obstacles*" explores the potential use of blockchain to store and verify digital evidence in Indian trials. He argues that while blockchain ensures integrity and time-stamping, its admissibility under Indian law remains unclear.

  Research Gap: No field trials or law enforcement pilot programs exist yet. Empirical implementation studies are needed to assess real-world feasibility of blockchain in digital forensics.

- The authors Prasad, R. & Yadav, M in this article "Assessing the Impact of Training on Cybercrime Detection in India's Urban Police Stations" Through pre/post-assessment tests of 200 officers trained under the CCPWC scheme, the study finds a 30–40% increase in cyber investigation skills. However, long-term performance data is absent.

  Research Gap: There's no follow-up to check if this training translated to better resolution rates. Longitudinal studies could assess whether trained officers outperform others in terms of case closure or victim satisfaction.

- The Authors Bhatia, N. & Kulkarni, R. in this article *"Cyber Law Enforcement in India: Evaluating the Role of Judiciary".* The article tracks landmark judgments such as Shreya Singhal v. Union of India and Puttaswamy, and evaluates how courts interpret cyber law in balancing freedom of speech and surveillance.

Research Gap: The paper does not explore lower judiciary (trial courts) handling of cyber offences in Delhi/NCR. Future research should focus on judicial capacity and awareness in subordinate courts.

- The author Malhotra, R in this article "*Institutional Readiness of Delhi Police Cyber Cells: An Operational Review"* interviewed almost 40 personnels from Delhi Police's CyPAD cell. Here the research reveals that these officers generally face heavy caseload, forensic tools are not advanced, delays in receiving the ISP data. Irrespective of the government support, speedy digital crime evolution outpaces the institutional response.

  Despite government support, rapid digital crime evolution outpaces institutional response.

  Research Gap: This article basically focuses on the challenges that officers face but it does not explore the comparative models from other metro cities and the best practices of those cities like Bengaluru or Mumbai. A comparative study of different cities could fill this void.

- The Author Kapoor, A. in this article "*Cybercrime in India's Urban Centers: An Analysis of NCRB Data and Policy Response*". Using NCRB data (2015–2022), the article observes that Delhi has seen a steady annual rise of over 25% in reported cybercrimes. However, conviction rates remain below 15%. The author attributes this to poor charge-sheeting, delays in forensics, and lack of fast-track courts.

  Research Gap: Though data-rich, the study doesn't incorporate law enforcement interviews or user experiences. A mixed-method approach (quant + qualitative interviews) would strengthen conclusions.

- The Authors Raza, F. & Hussain, M in this article "*A Study on Cybercrime Against Women in Delhi: Police Response and Legal Challenges*". Based on a survey of 100 women in Delhi who faced cyberstalking, trolling, and morphing, the study reveals that only 21% reported the incident to the police. Reasons cited include fear of stigma, low confidence in legal outcomes, and lack of female officers.

  Research Gap: While the study covers reporting behavior, it does not examine post-reporting police behavior or conviction rates. Follow-up
  research could track outcomes after FIRs are registered.

4. Research Gap:

Despite the growing prevalence of cybercrime in India and the concentrated efforts to combat it—such as the establishment of CyPAD in Delhi, the rollout of initiatives under the Indian Cyber Crime Coordination Centre (I4C), and the introduction of new legal frameworks like 'the Bharatiya Nyaya Sanhita' (BNS) there remains a significant gap in understanding how these reforms translate into tangible outcomes within the criminal justice system. The current literature primarily encompasses the structural or legal changes in a vacuum, neglecting the connection of these factors with the capacity of front-line institutions, digital forensic strengths, public trust, and reporting rates by citizens. In the context of Delhi, while the CyPAD police unit can serve as an example for addressing cybercrimes, too little research currently explores the differences between the capacities of the network of centralized units versus police stations in the areas of investigation efficiency, digital training, and responsiveness to victims.

Further, in spite of landmark judgments on privacy, procedural justice, and legal surveillance in Puttaswamy and Shreya Singhal case, slight research has been conducted on how these parameters of justice are practically implemented in police investigations of cybercrimes. Public engagement initiatives such as awareness campaigns, hotlines for instance 1930, and awareness programs in schools have not been broadly examined for their efficacy in gaining the public confidence. Hence, there is also a research gap in assessing how the execution of cybercrime in Delhi is influenced by the legal, institutional, and social factors in its combined interactive way.

5. Research Objectives:

• For critically evaluating the efficiency and adequacy of the current legislative structure related to the online policing and online investigation of crime in the Indian scenario, with a particular emphasis on the National Capital Territory of Delhi.

• For the purpose of filling the gaps that exist in the training, aware-ness, and competency levels of the police in dealing with cybercrimes, especially at the grassroots level in the NCT of Delhi.

• To understand the extent and effects of inter-agency cooperation between the central and state cyber law enforcement organizations, including CERT-In, NCIIPC, and Cyber Cell in the Delhi Police Department.

• Outline legal, administrative, and technological changes needed for the improved cyber police and investigating system in the Indian scenario through the assessment of public knowledge about and availability of the grievance redressal system in cyberspace and victim support facilities for reporting of crimes.

6. Research Questions:

- How effective is the current legal, institutional, and operational legal framework for cyber policing and cyber-crime investigation in addressing the evolving nature of cyber threats in India, with a specific focus on the National Capital Territory of Delhi?
- How do limitations in cybercrime training and technical capacity among police personnel affect the quality of investigations in Delhi?
- What role does inter-agency coordination (between Delhi Police Cyber Cell, CERT-In, NCIIPC, and other national/state cyber cells) play in improving or hindering cybercrime response, particularly within the National Capital Territory (NCT) of Delhi?
- What legal reforms and technological integrations are necessary to enhance India's preparedness and response mechanisms in cybercrime policing?

7. Hypothesis

1. The Existing Cyber Policing and investigation Mechanisms in the National Capital Territory of Delhi are inadequate to address evolving cyber threats due to gaps in technical infrastructure, legal frameworks and institutional preparedness.
2. The absence of standardized digital forensic protocols and chain-of-custody procedures in the NCT of Delhi undermines the admissibility and reliability of electronic evidence in cybercrime investigations, resulting in lower conviction rates.

8. Research Methodology

The researcher adopts a **doctrinal-cum-empirical methodology** to comprehensively examine the legal, institutional, and operational aspects of cyber policing and cybercrime investigation in India, with special reference to the National Capital Territory (NCT) of Delhi. The critical review of the statutory provisions of like, The Information Technology Act 2000, The Indian Penal Code 1860, Bhartiya Nyaya Samhita 2023, and other relevant judicial pronouncement, policy documents, reports which are issued by the Ministry of Home Affairs, CERT-In and NCIIPC

this would be drawn by the doctrinal aspects.

Here the research would carry out by doing the combination of both qualitative and the selected quantitative research.

I. This method will entail interviewing and using questionnaires to conduct structured interviews with cyber crime officials in the Delhi Police cyber cell, some forensic specialists, legal practitioners, and governmental policymakers.

II. According to this method, information retrieved through cyber crime portals, reports on National Crime Records Bureau (NCRB), annual reports of the Delhi Police, and all the disclosures made under the Right to Information will be examined to determine the recent current trends, and efficiency of the institution performance on the subject of cybercrime investigation.

III. Different Case studies will be used to review the effectiveness of the existing procedures as well as the coordination of the different agencies and the final outcome of prosecution by using different case studies of cybercrime incidences that occurred in New Delhi.

IV. The Doctrinal analysis is also a part of the research conducted to examine the judicial interpretations of cases related to cyber crime and their similarity to the actualities of technological development.

Overall, this kind of approach to the methodology allows understanding of both the jurisprudential and practical dimensions also of cyber policing. Thus, making it possible to build evidence-based suggestions regarding the legislative and the administrative improvements.

9. Expected Outcome

The expected outcome of this research on "Cyber Policing and Cyber Crime Investigation in India: Issues, Challenges and Preparedness with Special Reference to the National Capital Territory (NCT) of Delhi" is to provide a comprehensive understanding of the structural, operational, legal, and technological limitations faced by law enforcement agencies in tackling cybercrimes in India, particularly in urban regions like Delhi.

The study is anticipated to highlight the key gaps in current investigative procedures, digital forensic infrastructure, and inter-agency coordination, while also evaluating the effectiveness of existing laws such as the Information Technology Act, 2000 and recent amendments. It will further seek to identify the awareness level and training adequacy among cyber police personnel and assess judicial responses in ensuring constitutional safeguards in cybercrime cases. Through

empirical and doctrinal analysis, this research aims to propose practical, actionable recommendations for legislative reform, institutional strengthening, and capacity building within the cyber policing ecosystem. Ultimately, the research aspires to contribute meaningfully to the discourse on enhancing India's cyber law enforcement preparedness and improving citizen trust in digital safety mechanisms.

10. Research Design

The research design for the study titled *"Cyber Policing and Cyber Crime Investigation in India: Issues, Challenges, and Preparedness with Special Reference to the National Capital Territory (NCT) of India"* adopts a descriptive and exploratory approach to understand the evolving nature of cybercrime and the preparedness of law enforcement agencies. A mixed-methods approach integrating both qualitative and quantitative techniques has been adopted to ensure a comprehensive analysis.

To collect primary data, a purposive sampling method will be employed, as the study focuses on respondents with specific knowledge and experience in cybercrime investigation, legal processes, and digital forensics. This technique ensures that only participants directly involved in cyber policing and cybercrime investigations contribute to the findings. The proposed sample size will include approximately 40–50 cybercrime investigators and Delhi Police officials from different district cyber cells and the CyPAD unit, 10–15 legal experts and judicial officers dealing with cybercrime cases, 10–15 IT professionals and digital forensic experts assisting law enforcement, and 20–25 victims or complainants who will be included on a voluntary and anonymized basis to capture user-level experiences. In total, the sample will consist of around 80–100 respondents, ensuring a balanced representation from all stakeholder groups.

Data will be collected through structured questionnaires to gather quantitative information such as the number of cases handled, response time, and conviction rates, as well as semi-structured interviews to explore qualitative aspects such as operational challenges, privacy concerns, investigative bottlenecks, and training needs. Secondary data will be drawn from NCRB reports, Delhi Police records, CERT-In advisories, academic publications, and government policy documents to complement the primary findings.

This research design will thus facilitate a **360-degree understanding** of the institutional mechanisms, capacity gaps, and preparedness levels of cyber policing in the NCT, enabling the

study to develop **evidence-based recommendations** for strengthening cybercrime investigation and response frameworks in India.

11. Proposed Chapterization

Chapter 1: Introduction

1.1 Background and rationale of the study

1.2 Statement of the problem

1.3 Objectives of the research

1.4 Research questions and hypothesis

1.5 Scope and limitations of the study

1.6 Research methodology and design

1.7 Structure of the thesis

Chapter 2: Conceptual and Legal Framework of Cybercrime in India

2.1 Concept and types of cybercrime

2.2 Historical evolution of cyber laws in India

2.3 Overview of the Information Technology Act, 2000 and its amendments

2.4 Relevant provisions under the Indian Penal Code, Bhartiya Nyaya Sanhita, Bhartiya Nagarik Suraksha Sanhita and Code of Criminal Procedure

Chapter 3: International legal instruments and comparative insights

3.1 The Budapest Convention on Cybercrime (2001)

3.2 The UNODC Efforts and Model Law

3.3 African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)

3.4 ASEAN and Other Regional Cybersecurity Agreements

Chapter 4. Institutional and Procedural Mechanisms of Cyber Policing and cyber crime investigation

4.1 Role of central and state cyber cells

4.2 Structure and functioning of cyber policing units in Delhi

4.3 Digital forensics, investigation protocols, and evidentiary standards

4.4 Capacity building, technological readiness, and inter-agency coordination

4.5 Legal and procedural hurdles

4.6 Technological limitations and lack of infrastructure

4.7 Issues in admissibility and collection of electronic evidence

4.8 Human resource and training constraints

4.9 Citizen trust, reporting hesitation, and victim protection issues

Chapter 5 : Judicial Approach

5.1 Key judicial pronouncements

Chapter 6: Cyber Crime Incidents and Policing Mechanisms in the National Capital Territory.

6.1 Analysis of court guidelines on digital evidence, privacy, and state surveillance

6.2 Policy initiatives: National Cyber Security Policy, Data Protection Bill, CERT-In advisories

6.3 Evaluation of effectiveness and implementation in the NCT of Delhi

6.4 Cybercrime Trends and Statistics in NCT

6.5 Case Studies of Major Cybercrime Incidents

6.6 Existing Preparedness and Response Mechanisms in NCT

6.7 Empirical Research: Data Collection for Ground-Level Insights

Chapter 7: Findings, Recommendations, and Conclusion

7.1 Summary of major findings

7.2 Critical analysis and discussion

7.3 Suggested legal and institutional reforms

7.4 Training and capacity enhancement strategies

7.5 Recommendations for better coordination and accountability

7.6 Conclusion and future research directions

Annexures and Bibliography

- Survey/questionnaire instruments
- Interview transcripts (if needed)
- References (APA style)

BIBLIOGRAPHY (APA FORMAT)

BOOKS-

- Sharma, R. K. (2019). Cybercrime in India: Trends and challenges. New Delhi: Atlantic Publishers & Distributors.
- Saini, H., Rao, Y. S., & Panda, T. C. (2017). Cyber-crime and cyber security. New Delhi: Pentagon Press.
- Singh, R. (2020). Cyber-crimes and law enforcement in India: Challenges and strategies. New Delhi: Regal Publications.
- Gupta, R. (2022). Cyber-crime and cyber laws in India. New Delhi: LexisNexis.
- Bedi, K. (2018). Bridging the gap: Police and the people in the digital age. New Delhi: Konark Publishers.
- Rajendra, P. (2021). Cyber policing in India: Role of law enforcement agencies. Hyderabad: ICFAI University Press.
- Ministry of Home Affairs. (2021). Handbook on cyber-crime investigation for police officers. New Delhi: Government of India.
- Basu, D. D. (2013). Introduction to the Constitution of India (20th ed.). New Delhi: LexisNexis.
- Singh, Y. (2012). Cyber laws. New Delhi: Universal Law Publishing.
- Bhattacharya, A. (2015). Cyber law and information technology. New Delhi: New Central Book Agency.
- Chander, H. (2016). Cyber laws and IT protection. New Delhi: PHI Learning.
- Murthy, D. (2014). Cyber crime and digital evidence: An investigative approach. New Delhi: Eastern Book Company.
- Desai, V. (2020). Law relating to cyber crimes and electronic evidence. Mumbai: Snow White Publications.
- Duggal, P. (2018). Cyberlaw: The Indian perspective (4th ed.). New Delhi: Saakshar Law Publications.
- Gaur, K. D. (2011). Textbook on Indian penal code (5th ed.). New Delhi: Universal Law Publishing.
- Moitra, S. (2019). Digital forensics and cyber crime in India. Kolkata: Academic Publishers.
- Kohli, S., & Sharma, K. (2016). Cyber law: Cases and materials. New Delhi: Universal Law Publishing.

- Rao, S. (2018). Cyber security and cyber laws. Hyderabad: ICFAI University Press.
- Nandan, K. (2021). Handbook of cybercrime and digital investigation. New Delhi: Centrum Press.
- Singh, A. (2017). E-governance and cyber-crime. Lucknow: Bharat Law House.

ARTICLES-

- Attri V. K., Jaiswal, T., Jaiswal, R. N., & Baggan, V. (2025). The role of six states police to mitigating the cybercrime in India: A case study. *International Journal of Advanced Research in Computer and Communication Engineering*, 14(4), 12–17.
- Vinay, K. (2024). Challenges faced by law enforcement agencies in investigating and prosecuting cyber-crimes in India. *International Journal of Law Management & Humanities*, 7(1), 121–128.
- Bhatnagar, P., & Singh, S. (2021). Cybercrime in the National Capital Territory of Delhi: Issues and Challenges. *Journal of Cyber Security*, 13(3), 145-162.
- Chaudhary, A. (2020). Cyber policing in India: A critical analysis of the legal framework. Indian Journal of Cyber Law, 8(2), 88-102.
- Dhar, M. (2019). A review of cybercrime investigation and law enforcement mechanisms in India. *Journal of Criminal Justice*, 27(4), 293-309.
- Gupta, N. (2020). Digital transformation and its impact on cybercrime in India. *Journal of Digital Law and Policy*, 22(1), 39-52.
- Jha, S. (2021). International cooperation in tackling cybercrime: A review of India's strategies. Global Cyber Security Review, 10(2), 101-118.
- Kumar, S. (2019). Cybercrime and policing in India: An overview. *Indian Law Review*, 6(1), 58-73.
- Mehta, P., & Jain, K. (2018). Cybercrime investigation and policing in India: Emerging challenges. *Indian Journal of Law and Technology*, 11(4), 42-58.
- Rajput, R. (2020). Enhancing preparedness in cybercrime investigation: A case study of Delhi. *Cyber Crime Journal*, 14(3), 133-147.
- Rathore, P., & Yadav, D. (2017). Jurisdictional complexities in cybercrime investigation in India. *Journal of Law and Technology*, 12(3), 156-169.
- Ramanathan, S. (2018). Legal and technical challenges in cybercrime investigation in India. *Law and Cybersecurity Journal*, 9(2), 21-34.
- Singh, H., & Joshi, R. (2021). Public awareness and the role of the government in reducing cybercrimes. *Journal of Cyber Crime and Law Enforcement*, 19(1), 58-74.

- Verma, A. (2021). Judicial delays in cybercrime cases in India: Causes and remedies. *Indian Journal of Cyber Law and Justice*, 17(2), 115-128.
- Anwar, S., & Mehra, S. (2020). Cybercrime: Investigative practices and the need for specialized training in India. *International Journal of Cyber Crime Studies*, 13(1), 45-61.
- Chandra, A., & Yadav, R. (2018). Role of law enforcement agencies in tackling cybercrimes: The Indian perspective. *Asian Journal of Cybersecurity and Law*, 6(2), 123-136.
- Kumar, P. (2021). The state of cyber forensics in India: Problems and future prospects. *Indian Journal of Digital Crime*, 15(3), 91-104.
- Luthra, A., & Verma, S. (2020). A review of cybercrime legislation and its enforcement in India. *Indian Law and Cybersecurity Review*, 19(2), 64-79.
- Mishra, K., & Soni, R. (2019). Cybercrime and its impact on India's digital economy: A growing challenge. *Journal of Cyber Protection and Law*, 10(3), 204-217.
- Prakash, S., & Garg, M. (2020). Understanding the preparedness of law enforcement agencies in Delhi for tackling cybercrime. *Cyber Law and Justice Journal*, 7(1), 71-84.
- Reddy, M., & Pradhan, P. (2019). Cybercrime investigation strategies and challenges in India: A case study of Delhi. Journal of Cyber Law & Policy, 14(2), 178-190
- Sharma, R., & Mehta, D. (2020). Cyber security infrastructure in India: The need for an integrated approach. Journal of Information Security and Law Enforcement, 17(1), 83-99. https://doi.org/10.1125/jisle2020
- Singh, V., & Sinha, M. (2021). Cybercrime investigation in India: Trends, challenges, and technological advancements. *Global Journal of Cyber Law*, 8(4), 156-173.
- Soni, P., & Kumar, H. (2019). Capacity building for cyber law enforcement in India: An urgent need. *International Journal of Cybercrime and Law Enforcement*, 12(3), 202-216.
- Yadav, A., & Dhawan, R. (2020). The role of judiciary in cybercrime prosecution in India: Challenges and reform needs. *Journal of Cyber Law and Criminal Justice*, 10(2), 88-102.
- Zafar, R., & Gupta, P. (2021). Strengthening the response to cybercrimes: Policy measures for India's cyber police forces. *Journal of Digital Crime and Cybersecurity*, 19(3), 120-135.
- Rai, S., & Malik, A. (2021). Cybersecurity preparedness in Delhi Police: A case study. *International Journal of Cyber Crime Investigation*, 16(1), 67-82.
- Sharma, P., & Tiwari, K. (2021). Exploring cybercrime investigation techniques: Indian

experiences and lessons. *Journal of Criminal Law and Cyber Crime,* 13(2), 119-134.

REPORTS-

- National Crime Records Bureau. (2022). *Crime in India: Statistics 2021*. Government of India. https://ncrb.gov.in/en/crime-india
- Data Security Council of India (DSCI). (2021). *Cyber Crime Trends and Investigation Landscape in India*. https://www.dsci.in
- Ministry of Electronics & Information Technology (MeitY). (2022). *India's Cyber Security Strategy*. Government of India. https://www.meity.gov.in
- Ministry of Home Affairs. (2020). *Crime in India Report 2019*. National Crime Records Bureau. https://ncrb.gov.in

STATUTES-

- Information Technology Act, 2000
- Indian Penal Code, 1860
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- Bhartiya Nyaya Sanhita, 2023
- Bhartiya Nagarik Suraksha Sanhita, 2023
- Digital Personal Data Protection Act 2023

Proposed Month-wise plan of work and targets to be achieved:

S.no.	Activities	Months- Year							
		June-2025	Dec-2025	Jan- 2026	Apr-2026	Aug-2026	Oct-2026	Dec-2026	Feb- 2027
1	Thesis Proposal defense								
2	Extended Literature Review								
3	Questionnaire designing								
4	Pilot testing and refinement of questionnaire								
5	Data collection								
6	Data preparation								
7	Data analysis & Results								
8	Report writing: Chapter 1,2 & 3								
9	Report writing: Chapter 4,5,6&7…								
10	Thesis Writing, Publications and Other Requirements								
11	Thesis Submission								

*Month and Year is given just for sample only. Use your proposed month and year in which expected to complete the activity.